La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad

Lic. Virginia Ibarra – Lic. Mónica Nieves

Resumen

La seguridad hemisférica hoy es multidimensional. Fenómenos como la transnacionalidad, el terrorismo, la tecnología, Internet no solo han eventualmente signado la agenda internacional de estos tiempos, sino que resumen en materia de ciberseguridad una característica sustancial de la sociedad internacional, y por tanto un foco de análisis trascendente para las Relaciones Internacionales.

Con el inicio de la Guerra Fría se comenzó en Latinoamérica la construcción del sistema interamericano, que a instancias del Tratado Interamericano de Asistencia Recíproca (TIAR), la Organización de Estados Americanos (OEA) y bajo el patrocinio de Estados Unidos como potencia hegemónica occidental, fueron cimentando una noción de seguridad particular para la región. Desde el nacimiento de la Junta Interamericana de Defensa (JID) en 1942 hasta la Declaración de Bridgetown en 2002, la noción de "Seguridad Hemisférica" emanada de aquel sistema ha sufrido una notoria evolución.

A partir de la Conferencia Especial de Seguridad de México de 2003, los Estados miembros de la OEA acordaron ampliar el concepto de seguridad, adoptando un enfoque multidimensional, lo que ha permitido abrir un dilatado abanico de nuevas amenazas y riesgos. Particularmente -teniendo como antecedente fundamental los trabajos de la Convención Interamericana contra el Terrorismo de 2002-, se ha asumido al terrorismo y a los ataques a la seguridad cibernética como parte de estos nuevos flagelos. En este sentido, la OEA desde la Comisión Interamericana contra el Terrorismo (CICTE) ha generado distintas instancias a fin de cohesionar la participación de los gobiernos, del sector privado y de la sociedad civil en pos de la identificación de las necesidades nacionales de seguridad cibernética y la formulación de políticas específicas.

El mundo está conectado digitalmente. Con el propósito de resguardar la libertad y asegurar el ejercicio pleno de los derechos de los ciudadanos, el Estado depende y se apoya inevitablemente en la tecnología. Entre otros atributos soberanos, la vigilancia estatal condiciona su efectividad a los recursos tecnológicos disponibles. Es en este punto, que desde un abordaje específico de las

Relaciones Internacionales y posicionando al Estado jerárquicamente como actor internacional, que se hace necesario determinar qué lugar ocupa el terrorismo en la construcción conceptual de la ciberseguridad, en el marco de la multidimensionalidad de la seguridad hemisférica del Siglo XXI.

Este artículo pretende identificar el desafío que se le presenta al Estado, sorteando los obstáculos que le anteponen actores transnacionales desde dos frentes: por un lado el ilegal, con el terrorismo y su expresión cibernética, y por otro lado desde el sector privado que actualmente domina en gran medida el acceso a Internet, y por ende se adueña de la mayor parte de la información en línea. Asimismo, se pretende identificar a modo de ejemplo, las principales líneas de trabajo que desde el Estado uruguayo se han generado como planes de protección de la información.

Palabras clave: Terrorismo, Ciberseguridad, Estado, Transnacionalidad

El camino de la multidimensionalidad

La seguridad no es un tema nuevo. Habría que mirar muchos siglos atrás para encontrar el primer abordaje filosófico del tema -en un sentido amplio más allá de la garantía del cuidado físico- de la mano de Thomas Hobbes, quien la consideró una de las causas del nacimiento del Estado moderno, como encargado de proteger al individuo y velar por la satisfacción del bienestar general[1].

Más acá en el tiempo, desde los 90's el concepto de seguridad se ha transformado incesantemente, lo que determina que no solo deban identificarse los elementos de cambio y los que permanecen -en tanto hacen a la naturaleza del concepto-, sino que se requiere una especial atención sobre su objeto y alcance.

La seguridad tanto interna como externa, hacen a la esencia del Estado desde su conformación. La seguridad fue, es y será un objetivo ineludible en la actuación del Estado, a pesar de que su significado y alcance se hayan modificado al compás de las transformaciones de la sociedad internacional.

Desde el nacimiento de la JID en 1942 hasta la Declaración de Bridgetown en 2002, la noción de "Seguridad Hemisférica" emanada de aquel sistema ha sufrido una notoria evolución. Con el inicio de la Guerra Fría se comenzó en Latinoamérica la construcción del llamado Sistema

1 Ampliar en “Leviatán: o la materia, forma y poder de una república eclesiástica y civil”.

Interamericano, que a instancias del TIAR, la OEA y bajo el patrocinio hegemónico de Estados Unidos como potencia occidental, fueron cimentando una noción de seguridad particular para la región. En pocas palabras construyeron una arquitectura de seguridad a imagen y semejanza de la bipolaridad que se vivía.

En la actualidad, la seguridad como elemento político clave en la escena internacional, se compone de nuevas dimensiones que se suman a las consideradas tradicionales, como son la militar y la política. En ese sentido, van paulatinamente adquiriendo relevancia las facetas económica, la científica-tecnológica-comunicacional, la medioambiental, la social-cultural-étnica, la ilegal -narcotráfico,delito cibernético, el tráfico de personas, el lavado de activos,etc.- la alimentaria, entre otras. En estos términos, es fácil percatarse que las políticas públicas de los Estados -cada vez más impregnadas por la variedad de elementos que hacen a la seguridad-, están obligadas a acompañar los cambios impuestos por una pléyade cada vez más amplia de riesgos.

Luego de los atentados de Nueva York del 11 de setiembre de 2001 (11-S) y el terrorismo determinado como una de las prioridades de la seguridad nacional de Estados Unidos, se "re-orientaron sus prioridades en términos de prevención de conflictos y de la construcción de paz", y la OEA inició el camino de la multidimensionalidad de la seguridad (Serbin, 2010: 20).

Fenómenos como la transnacionalidad, el terrorismo, la tecnología, Internet no solo han eventualmente condicionado la agenda internacional de los últimos tiempos, sino que resumen en materia de ciberseguridad una característica sustancial de la sociedad internacional. La idea de la Sociedad de la Información, en la que es de orden la noción de autodeterminación en línea en términos de la libertad informática del individuo, implica contemplar elementos como conexión a la Red, software, el dominio de la tecnología por las grandes corporaciones, el rol del propio Estado en términos de defensa de un derecho humano como es el acceso a Internet, entre otros.

En 2002 fue aprobada en el seno de la OEA, la Convención Interamericana contra el terrorismo, cuyo objetivo es "prevenir, sancionar y eliminar el terrorismo. Para tal efecto, los Estados Parte se comprometen a adoptar las medidas necesarias y fortalecer la cooperación entre ellos, de acuerdo con lo establecido en esta Convención" (AG/RES.1840 (XXXII-O/02)

En la Declaración de Bridgetown de 2002, los Estados miembros de la OEA concilian una Seguridad Hemisférica, e incluyen un enfoque multidimensional en el que reconocen: "(...) que las amenazas, preocupaciones y otros desafíos a la seguridad del hemisferio son de naturaleza diversa y alcance multidimensional y que el concepto y enfoque tradicionales deben ampliarse para abarcar amenazas nuevas no tradicionales, que incluyen aspectos políticos,económicos, sociales, de salud, ambientales".(Declaración de Bridgetown, 2002)[2].

En Barbados se acuerdan las modificaciones que se formalizarán en la Declaración sobre Seguridad en las Américas de la Conferencia Especial de Seguridad de México de 2003, en la que se amplía el concepto de seguridad hemisférica aplicando el encuadre multidimensional, y colocando su eje en la protección de la persona humana. Comenzará entonces a cimentarse una "arquitectura flexible de seguridad". Existe consenso académico en que el fin de la Guerra Fría marcó una perspectiva de defensa hemisférica diferente a la de los años cuarenta.

Sobre el análisis de la Declaración sobre Seguridad en las Américas de 2003 en que se listan no taxativamente lo que se consideran "nuevas amenazas, preocupaciones y otros desafíos de naturaleza diversa", Armerding (2003) entiende que en realidad la denominación "nuevas amenazas" debiera corresponder a "amenazas no tradicionales" y pone como ejemplo el terrorismo, el narcotráfico y el crimen organizado. Afirma que a pesar de haber cierta aquiescencia sobre la denominación, no son fenómenos "estrictamente" nuevos en la región. Lo que puede realmente considerarse nuevo es el contexto mundial globalizado, algunos actores internacionales, la tecnología para transmitir sus efectos y la "multiplicación de sus consecuencias".

"Lo novedoso de dichos fenómenos entonces, no es su existencia, sino el hecho de que se han transnacionalizado, y han asumido una magnitud y un alcance que trascienden las previsiones y pautas con que tradicionalmente se enfocan las cuestiones de seguridad interior, defensa nacional y seguridad internacional." (Armerding, 2006: 3).

El terrorismo constituye desde la óptica de las Relaciones Internacionales un típico asunto interméstico, en tanto refiere a un tema considerado simultáneamente interno y externo. La inclusión de esta perspectiva que va más allá de una mirada militar a los asuntos de seguridad, marca un punto de quiebre en la evolución hacia la multidimensionalidad de la seguridad.

2 AG/DEC. 27 (XXXII-O/02)

Terrorismo en la historia, en el mundo y en la región

En cuanto al término terrorismo a nivel internacional, abundan en la academia infinidad de definiciones y tipologías. Una de las posiciones, sostiene que al tratarse de un fenómeno que se consolida en el Siglo XXI como un actor más del sistema internacional, debería precisarse una definición "mínima" que lo identifique con el fin de implementar políticas que permitan combatirlo. Por otra parte, hay una postura que sugiere evitar el uso de la palabra terrorismo por motivos intrínsecos - de definición, extensión, comprensión y manipulación-, y por motivos geopolíticos ya que puede suponer colaboración con un Estado. Esta perspectiva considera que cada ataque perpetrado es único y debe ser estudiado según el origen y peculiaridad del mismo. El grupo y móvil del ataque del 11-S no fue igual al de la matanza de Atocha, ni a los consumados por Boko Haram. Los instrumentos de prevención y contención también deben ser planteados según el caso, no se implementan de la misma forma con una entidad transnacional que con una sub-estatal, y tampoco tienen los mismos problemas de prevención que el terrorismo de Estado. Es un fenómeno complejo para el cual no hay una respuesta univoca. Este hecho plantea la duda de si es recomendable para su entendimiento y combate acotarlo a un solo término. De todas maneras, independiente de que exista o no una definición convenida, existen ciertas variables básicas presentes en determinados hechos que indican fehacientemente que se está ante un acto de terrorismo.

Para la Real Academia Española el terrorismo se define como: “Dominación por el terror - Sucesión de actos de violencia ejecutados para infundir terror.-Actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos”.

La definición que cita el Índice Global del Terrorismo reconoce que no es solo el acto físico de un ataque, sino también el impacto psicológico que tiene en una sociedad durante muchos años, y lo califica como: “la amenaza o uso real de una fuerza ilegal y de violencia por parte de un actor no estatal para alcanzar un objetivo político, económico, religioso o social mediante el miedo, la coacción o la intimidación”[3].

3 Global Terrorism Index, 2015. Disponible en: http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf

Mientras en el siglo XVIII, durante la Revolución Francesa, Robespierre encumbró el terror como forma de alentar el movimiento revolucionario -momento en que se escucha por primera vez *terrorisme*-, el cual se aplicará después a lo que se llamará terrorismo de Estado. Hoy el terrorismo se ha transformado en un actor omnipresente del sistema internacional. Este fenómeno ha acompañado los procesos de crisis, y los cambios estructurales de la sociedad internacional mutando conforme esta evoluciona.

Desde otra perspectiva, visto como un acto contra el Estado, su uso se extendió durante el siglo XIX bajo la forma de mensaje, a fin de promover cambios en la estructura política y social de la época. El grupo populista ruso, Narodnaya Volya, creado en oposición a la monarquía zarista en 1878 es un ejemplo de ello.

Siguiendo su evolución el Siglo XX ofrecerá un escenario donde esta clase de actos adquirirán una relevancia particular. La primera década presencia el atentado terrorista de Sarajevo -en el que un joven perteneciente a la organización "Mano Negra" da muerte al heredero de la corona austro-húngara- , un hecho que adquirió una connotación política de tal magnitud que lo convirtió en el detonante final que da paso a la Primer Guerra Mundial. En el transcurso de ese siglo, también se presenció un terrorismo de Estado exacerbado por diferentes ideologías, y en este sentido los ejemplos abundan, Italia Facista, Alemania Nacionalsocialista - Nazi-, el Stalinismo, los gobiernos dictactoriales del Cono Sur (Tortosa, 2005).

Finalizando el "largo siglo XX" al decir de Eric Hobsbawn, los actos de terrorismo acaecidos en América Latina generaron tal alarma en los gobiernos de la región que se abocaron a realizar una serie de reuniones en las que se comprometieron a “prevenir, combatir y eliminar el terrorismo”. De esta manera convocaron en 1994 a la Primera Cumbre de las Américas, en 1996 a la Primera Conferencia Especializada en Terrorismo -Declaración de Lima-, y en 1998 a la Segunda Conferencia Especializada en Terrorismo[4].

En 1999 con la adopción del "Compromiso de Mar del Plata" fue creado en el ámbito del sistema interamericano el CICTE[5], integrado por las autoridades nacionales competentes, su tarea consiste en preparar las acciones conjuntas en la lucha contra el terrorismo y coordinar sus modificaciones.

4 Comité Interamericano contra el Terrorismo. Disponible en: http://www.oas.org/es/sms/cicte/acerca_nosotros_historia.asp

5 AG/RES. 1650 (XXIX-O/99)

Semejante a la Comisión Interamericana para el Control del Abuso de Drogas (CICAD), el CICTE no dispone de una adecuada estructura burocrática y carece de influencia sobre los actores nacionales.

Es casi imposible negar los cambios trascendentes en la Política Internacional y en las Relaciones Internacionales que se generaron a partir del 11-S. Lo que durante la bipolaridad había sido "la guerra contra el comunismo", a partir de ese momento es sustituida por la "guerra contra el terror" encarnada en Al Qaeda y su transnacionalidad. Para Mary Kaldor la Guerra Fría y la "guerra contra el terror" se asimilan a "viejas guerras que incorporan el uso de las nuevas tecnologías". Esta práctica implica un gran problema para el mundo ya que enfrentar los conflictos actuales en virtud de las recetas arcaicas que confrontaron las guerras hasta mediados del siglo XIX, puede constituir un obstáculo para su resolución e "incluso podría exacerbarlos" (Kaldor, 2006: 12). De todas maneras, puede apreciarse que a raíz de los ataques terroristas en EE.UU., se adoptó un nuevo enfoque de los trabajos a nivel interamericano para hacer frente al terrorismo.

Reconociendo la transnacionalidad de los riesgos que afectaban la región, el Consejo Mercado Común (CMC) aprobó en 1999 el Plan General de Cooperación y Coordinación Recíproca para la Seguridad Regional en el MERCOSUR, la República de Bolivia y la República de Chile, en el que involucró a las Fuerzas de Seguridad y/o Policiales, a fin de propender a la generación de mecanismos de prevención y control en materia de seguridad. Identifica especialmente dentro del ámbito delictivo -entre otros- al terrorismo. Como parte del Plan General para la Seguridad Regional, se creó el Grupo de Trabajo Especializado sobre Terrorismo (GTE).

Incluir al terrorismo transnacional en la agenda de seguridad en MERCOSUR, fue una decisión que se tomó a raíz de los ataques contra la embajada israelí en Buenos Aires en 1992, y la Asociación Mutual Israelita Argentina (AMIA), en 1994. Aunque la mayor trascendencia del GTE fue resultado de la Declaración conjunta de los Ministerios de Interior y Justicia del Mercosur, el 28 de setiembre de 2001, en la que rechazaban los ataques terroristas del 11-S y anunciaban la extensión del trabajo conjunto en contra de las nuevas formas de la amenaza terrorista. A través de la modificación del Plan General para la Seguridad Regional, el GTE fue complementado por el Grupo de Trabajo Permanente, al que a partir de ese momento se encontrará subordinado (Flemes, 2004).

Además de casi una veintena de variados temas en los que puso su énfasis la Tercera Cumbre de las Américas en la ciudad de Québec en abril de 2001, su Plan de Acción incluyó la seguridad hemisférica y la lucha contra el terrorismo. A raíz de los atentados del 11S, el 21 de setiembre de 2001 en la XXIII Reunión de Consulta de Ministros de Relaciones Exteriores, se adoptó la Resolución para el Fortalecimiento de la Cooperación Hemisférica para Prevenir, Combatir y Eliminar el Terrorismo[6], condenando los ataques terroristas perpetrados, y recordando la Declaración de Principios de las Cumbres de las Américas de Miami, la de Santiago y la de Quebec. En 2002 se aprobó en el seno de la OEA -a impulso de Estados Unidos-, la Convención Interamericana Antiterrorista, en la que los Estados se comprometen a colaborar en la lucha contra el terrorismo.

Dentro del ámbito de acción militar en defensa -considerada un área básica y tradicional en el ejercicio soberano de un Estado- la lucha contra el terrorismo que se inició el 11-S, ya difícilmente distingue entre la seguridad interna y externa de un Estado. De hecho, la guerra contra el terrorismo se ha ampliado de tal manera que implica lo que Wæver (2009: 96) denomina "redes directas de apoyo", incorporando a la agenda de seguridad variados temas.

El yihadismo global reinventándose a través del ciberterrorismo, suma a la agenda internacional de seguridad actual, un nuevo reto a la sociedad de la información. El autodenominado "Ciber Ejército del Califato", rama de guerra cibernética del Estado Islámico, declaró estar preparado para provocar un Armagedón cibernético" con el fin de hacer colapsar infraestructuras informáticas críticas occidentales que sin duda afectarían nuestra región.

En respuesta a este escenario, en 2015 EEUU presentó su nueva política de ciberdefensa, una estrategia de disuasión que permite determinar el origen de toda agresión que provenga desde Internet de cara a proteger información sensible. Esta estrategia, ejecutada por el Comando Cibernético creado en el 2009 con objetivos ofensivos- defensivos, también contempla la posibilidad de ejecutar acciones defensivas, siempre y cuando, se haga para "proteger los intereses de Estados Unidos"[7].

6 Ampliar en: http://www.oas.org/es/sms/cicte/acerca_nosotros_historia.asp
7 Ampliar en: Es Global. Disponible en: http://www.esglobal.org/es-posible-un-pearl-harbor-cibernetico/

Resulta interesante recurrir al análisis de Kaldor (2001), en el que suma la noción de "guerras virtuales y del ciberespacio" en función de lo que califica como revolución en las relaciones sociales de la guerra, como consecuencia del desarrollo tecnológico.

Después de los atentados de París de 2015, varios Estados se abocaron a diseñar productos que les permitiera monitorear las comunicaciones de los extremistas. Según el profesor Peter Sommer, estos grupos yihadistas suelen identificar, y atraer a su causa, a desarrolladores de sistemas fáciles de usar. Cita como ejemplo SureSpot, un sistema que permite cifrar mensajes con facilidad dejando de lado el uso de sistemas que ofrecen las grandes corporaciones tecnológicas. Aún así las corporaciones juegan un rol importante en este combate facilitando a los Estados "metadatos". En esta línea el Reino Unido debate a nivel parlamentario el proyecto de instrucción Powers Bill, que permitirá solicitar a los proveedores de servicios de internet guarden metadatos durante un año. Esto no prohibiría el cifrado, pero obligaría a las empresas a renunciar a las claves de descifrado para que los mensajes codificados puedan ser leídos. Ante esta propuesta empresas como Facebook, Google, Microsoft, Twitter y Yahoo han expresado su preocupación ante el Parlamento sobre dicho proyecto, ya que consideran que significaría vulnerar la seguridad de sus productos, y trae a debate la vulnerabilidad del derecho de privacidad en internet (BBC, 2015)[8].

La concepción regional de la Ciberseguridad

La ciberseguridad es definida en líneas generales como la seguridad de la información digital almacenada en redes electrónicas, aunque aún hoy no hay un consenso en su definición. La noción de ciberseguridad debe distinguirse del concepto de seguridad de la información, ya que si bien generalmente refieren a lo mismo, este último apunta a la actividad de las organizaciones y profesionales de las tecnologías de la información, mientras que la ciberseguridad tiene un alcance más político o vinculado a la seguridad nacional (Comnimos, 2013).

Particularmente en esta dimensión de la seguridad, es de orden la colaboración entre el sector público y privado, es decir que junto al Estado deberán trabajar las corporaciones vinculadas de alguna manera a las tecnologías de la información, las ONG's y la sociedad civil. En junio de 2004 fue aprobada la Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad

8 Ampliar en: http://www.bbc.com/mundo/noticias/2015/11/151117_tecnologia_estado_islamico_comunicacion_lb

Cibernética de la OEA[9]. En ese marco, el Secretario de Seguridad Multidimensional de la OEA, Adam Blacwell, ha afirmado que "las autoridades deben promover la creación de una cultura de la seguridad cibernética", y para ello es necesario la colaboración de todas las partes interesadas a nivel nacional[10] (OEA, Symantec, 2014).

En este sentido, es paradigmática la Cumbre Mundial sobre la Sociedad de la Información (CMSI)[11] en la que se reunieron por primera vez en igualdad de condiciones en una cumbre de la ONU, actores públicos -Estados- y privados -empresas e individuos[12]. Entre las discrepancias que aparecieron en la fase de Ginebra en 2003 (Rodríguez: 2005; Ramonet: 2003) está aquella que versa sobre las libertades públicas, en lo que refiere al respeto de la privacidad de los usuarios de Internet, lo que las Ong's denuncian se fue deteriorando luego de los atentados del 11-S.

Como consecuencia del desarrollo en seguridad cibernética aparece un efecto poco deseado por los usuarios de Internet, y es la vigilancia sobre los ciudadanos que arremete contra el derecho a la privacidad. Mucho hacen los Estados en pos de la protección de la libertad de expresión en términos de bien común, promoviendo el acceso a Internet y las nuevas tecnologías, aunque se soslayan las consecuencias sobre el derecho a la privacidad (Nyst, 2013).

Al tradicional fin de vigilancia del Estado avivado por distintas amenazas reales o no, acompañado por la tecnología con capacidad de vigilar un mundo "hiperconectado" (Osaba, 2015: 9), se suma el poder que las grandes corporaciones vinculadas a la tecnología, ostenta con el dominio de la información en Internet. Esta situación conforma un escenario particular en el que un atributo esencial de la soberanía del Estado como es el de vigilancia, se ata a la decisión de actores transnacionales que han incrementado su poder a pasos agigantados, desde que se privatizó el uso de Internet.

En el marco de la OEA, en 2004 la Asamblea General de la OEA aprobó la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética[13] mandatando a la Secretaría del CICTE a entender sobre asuntos de Seguridad Cibernética. El programa de seguridad cibernética de la OEA contempla las particularidades de las amenazas cibernéticas para cada

9 AG/RES. 2004 (XXXIV-O/04)
10 Ver: Tendencias de seguridad cibernética en América Latina y el Caribe, .Informe 2014.
11 Realizada en dos fases: la primera en Ginebra en diciembre de 2003, y la segunda en Túnez en noviembre de 2005.
12 Ampliar en: http://www.itu.int/net/wsis/index-es.html
13 Ampliar en: http://www.oas.org/es/sms/cicte/programas_cibernetica.asp

Estado, así como las capacidades nacionales para enfrentarlas, promoviendo la participación directa de los gobiernos, el sector privado y la sociedad civil en la formulación de las políticas de seguridad cibernética. Con la aprobación de la "Estrategia Integral de Seguridad Cibernética Interamericana", la OEA se transformó en el primer organismo regional en adoptar una estrategia en esa materia.

En pos de la construcción de "capacidades de seguridad cibernética" entre los Estados Miembros, la Secretaría del CICTE utiliza un enfoque integral, para el que existe una responsabilidad nacional y regional en la materia, con la participación de variados actores públicos y privados, que desde lo político y lo técnico trabajarán para asegurar el ciberespacio[14].

En este contexto, surgen en a nivel nacional los Equipos de Respuesta a Incidentes (CSIRT) de "alerta, vigilancia y prevención" en materia de ciberseguridad. Se apunta a la creación de una red de alerta hemisférica que brinda formación al personal competente en la materia, de los distintos gobiernos de los Estados Miembros, buscando "promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio."[15]. Es fundamental la consideración de las particularidades de cada país, en el entendido de que las necesidades son diferentes, por ese motivo, la Secretaría del CICTE ha implementado un sistema de evaluaciones frente a la solicitud de asistencia técnica de un Estado Miembro, que permiten identificar los requerimientos nacionales a fin de instrumentar herramientas específicas que faciliten el fortalecimiento en la materia.

De acuerdo al Informe de 2014 de la OEA y Symantec sobre Tendencias de seguridad cibernética en América Latina y el Caribe, y en el entendido de que tanto usuarios, operadores y reguladores de Internet requieren de acceso a información "oportuna y precisa" a fin de hacer frente a las amenazas y vulnerabilidades cibernéticas, se ha intentado presentar el "ecosistema informático de América Latina y el Caribe"[16]. Es importante recalcar que en este sentido la OEA se ha enfocado en favorecer la cooperación entre el sector público, privado, académico y los usuarios finales, recalcando que los Estados deben promover una cultura de seguridad cibernética y actuar en pos de la protección de los usuarios individuales que en definitiva son los actores más vulnerables.

14 Ampliar en: http://www.oas.org/es/sms/cicte/programas_cibernetica.asp.
15 Ampliar en: http://www.oas.org/es/sms/cicte/programas_cibernetica.asp.
16 Ver en: Tendencias de seguridad cibernética en América Latina y el Caribe, Informe 2014.

A pesar de los esfuerzos, el Informe Ciberseguridad 2016 ¿Estamos preparados en América Latina y el Caribe? - colaboración entre el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford.-, demuestra que la región presenta vulnerabilidades "potencialmente devastadoras"[17].En palabras del Presidente del BID Luis Alberto Moreno: "Si los lectores han de llevarse un sólo mensaje de este Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, es que una enorme mayoría de nuestros países aún están poco preparados para contrarrestar la amenaza del cibercrimen" (BID-OEA, 2016: IX).

La experiencia uruguaya en Ciberseguridad

En consonancia con lo que ocurre a nivel internacional Uruguay ha avanzado sobre la legislación en la materia. Con la Ley 18.362 de 2008, se creó el "Centro Nacional de Respuesta a Incidentes de Seguridad Informática" (CERTuy) dentro de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). Esta agencia es la principal autoridad en seguridad cibernética del gobierno uruguayo. En tanto la responsabilidad primaria en la investigación de delitos cibernéticos y similares, depende de la Unidad de Delitos Cibernéticos de la Policía Nacional, que es asistido por CERTuy[18]

A partir del 2009, se faculta a AGESIC según el Decreto No. 451/009, y a través de CERTuy para proteger los sistemas informáticos que soporten activos de información críticos del Estado, así como los sistemas circundantes. En consonancia, y con el Decreto No. 452/009 se persigue la adopción de una Política de Seguridad de la Información, con el propósito de impulsar un Sistema de Gestión de Seguridad de la Información.

Con el impulso de la OEA, mediante su Iniciativa de Seguridad Cibernética, y por el Decreto 36/015 se implementó en Uruguay un escudo de seguridad DCSIRT (Centro de Respuestas a Incidentes de seguridad Cibernéticos) contra el ciberterrorismo, que actúa en red con organizaciones internacionales como CICTE, y la red de Ministerios de Defensa de UNASUR, y que funciona bajo la órbita del Ministerio de Defensa Nacional.

17 Ampliar en: http://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420.html

18 Ver en: Tendencias de seguridad cibernética en América Latina y el Caribe, Informe 2014.

De todas formas, el Informe Ciberseguridad 2016 -reveló que la preparación de Uruguay ante la amenaza del cibercrimen se encuentra en un nivel intermedio de madurez, pero aún lejos de países avanzados como Estados Unidos o Israel. La valoración de la "madurez" de las políticas de seguridad cibernética se realizó en base a 49 indicadores de cinco áreas, a saber: política y estrategia, cultura y sociedad, educación, marco legal y tecnología.

Algunas reflexiones

En términos de una agenda de seguridad del Siglo XXI, que se ha ido consolidando sobre la base de lo ocurrido tras los atentados del 11-S, la visión multidimensional de la seguridad hemisférica a la que se dio paso integra asuntos variados, con multiplicidad de potenciales actores que crecen en poder e indefinición. La seguridad está signada por fenómenos como la transnacionalidad, el terrorismo, la tecnología, Internet, resumiendo en materia de ciberseguridad una característica sustancial de la actual sociedad internacional, que como objeto esencial de estudio para las Relaciones Internacionales presenta nuevos desafíos.

Desde la OEA se ha intentado crear una nueva arquitectura de seguridad que acompañe el debate que se estaba dando a nivel internacional respecto al presente y el futuro de la seguridad en sus diversas modalidades, intentando cierta flexibilidad, e instrumentando diferentes espacios y políticas para dotar a los Estados Miembros de las capacidades para enfrentar las nuevas amenazas que trascienden los antiguos paradigmas de conflictividad inter-estatal típica del siglo pasado.

La multiplicación e importancia que han ido adquiriendo los actores transnacionales ponen en jaque no solo al rol del Estado como actor privilegiado de las Relaciones Internacionales, sino que presenta un panorama de incertidumbre sobre un futuro en el que cada vez es más patente que los primeros van ganando posiciones a consta de permear la preciada soberanía estatal.

Sobre la ciberseguridad hay mucho trabajo que hacer y uno de los desafíos más importantes es lograr un compromiso real de los Estados en la generación de políticas públicas específicas, y en la construcción de una cultura de ciberseguridad. Para alcanzar este objetivo, primero deben lograrse articulaciones y puntos de coincidencia desde las organizaciones internacionales afines, el sector público y privado, de manera de ofrecer a los Estados herramientas efectivas, tanto de protección y cuidado de los individuos, como de lo que se considera información crítica para los gobiernos.

Bibliografía

Armerding,G. (2006). Una mirada a la Declaración sobre Seguridad en lasAméricas. Centro Argentino de Estudios Internacionales. Programa Defensa y Seguridad. Disponible en: http://www.caei.com.ar/sites/default/files/14_3.pdf. Consultado: 15/09/2016

Del Arenal, C.(2002), La nueva sociedad mundial y las nuevas realidades internacionales: Un reto para la teoríay para la política. Cursos deDerecho Internacional y Relaciones Internacionales. Bilbao:Servicio .Editorial de la Universidad del País Vasco. pp.17-85. Disponible en: http://www.ehu.eus/cursosderechointernacionalvitoria/ponencias/pdf/2001/2001_1.pdf. Consultado: 10/05/2016

BBC, (2015) ¿Qué sabemos sobre las comunicaciones encriptadas que utiliza Estado Islámico? Disponible en: http://www.bbc.com/mundo/noticias/2015/11/151117_tecnologia_estado_islamico_comunicacion_lb. Consultado: 2/09/2016

Es Global, ¿Es posible un Pearl Harbor cibernético?(2015) Disponible en: http://www.esglobal.org/es-posible-un-pearl-harbor-cibernetico/ Consultado 2/09/2016

BID, Comunicado de prensa, 14 de marzo 2016, Disponible en:http://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420.html Consultado: 1/10/2016

Comnimos, A. (2013) Una agenda de ciberseguridad para la sociedad civil: ¿qué hay en juego?. En: Temas Emergentes. APC. Disponible en: https://www.apc.org/es/system/files/APCIssue_Cybersecurity_ES.pdf Consultado: 15/08/2016

El Estado Islámico lleva la guerra al ciberespacio y anuncia que hackeará Google, 2016, Recuperado de http://www.mil21.es/noticia/467/claves/el-estado-islamico-lleva-la-guerra-al-ciberespacio-y-anuncia-que-hackeara-google.html Consultado 01/10/2016

Flemes, D. (2004). Institution Building in Mercosul's Defence- and Security Sector (II). The Common Containment of Transnational Security Threats. En: Research Project: "Heading towards a regional Security AP 22. ISSN: 1611-0188. INSTITUTE FOR IBEROAMERICAN STUDIES. Hamburgo, Alemania. Disponible en: https://www.files.ethz.ch/isn/46976/arbeitspapiere22e.pdf Consultado: 10/07/2016

Global Terrorism Index, 2015 Disponible en: http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf Consultado en 12/06/2016

Nyst, C. (2013) El derecho a la privacidad y a la libertad de expresión: dos caras de la misma moneda. Cuestión de Derechos. Revista Electrónica. No 4 - primer semestre 2013 - ISSN

1853-6565. pp. 24-32. Disponible en: https://www.apc.org/es/system/files/ADC%20-%20Cuestion%20de%20derechos%20-%20Revista-numero4%20-%202013.pdf Consultado: 01/09/2016

OEA. Declaración de Bridgetown. Enfoque Multidimensional de la Seguridad Hemisférica. Disponible en: http://www.oas.org/xxxiiga/espanol/documentos/docs_esp/agcgdoc15_02.htm Consultado: 10/05/2016

OEA.Documentos Claves de la OEA sobre Seguridad Seguridad Nacional. I.OEA/Ser.D/XXV.. Secretaría de Seguridad Multidimensional. Disponible en: https://www.oas.org/csh/docs/Documentos%20Claves.pdf Consultado: 10/05/2016

OEA. Convención Interamericana contra el Terrorismo. Recuperado de: http://www.oas.org/es/sms/cicte/documents/AG%20RES%201840%202002%20espanol.pdf Consultado: 10/05/2016

OEA. Cooperación para la seguridad hemisférica. AG/RES.1123(XXI-O91). Recuperado de: http://scm.oas.org/pdfs/agres/ag03805S01.PDF Consultado: 10/05/2016

OEA. Fortalecimiento de la cooperación hemisférica para prevenir, combatir y eliminar el terrorismo. Disponible en: http://www.oas.org/es/sms/cicte/documents/doc_rc_23_res_1_01_spa.pdf Consultado: 10/05/2016

OEA. Tratado americano de soluciones pacíficas "Pacto de Bogotá".Disponible en: http://www.oas.org/juridico/spanish/tratados/a-42.html Consultado: 10/05/2016

OEA. Tratado Interamericano de Asistencia Reciproca. Disponible en: http://www.oas.org/juridico/spanish/tratados/b-29.html Consultado: 10/05/2016

Osaba, J. (2015) "La distopía ya está aquí: Vigilancia estatal de Orwell a Snowden y el guardián" En: Revista Dixit, no. 23, pp. 05–15, julio-diciembre 2015.

Kaldor, M. (2006). Un nuevo enfoque sobre las guerras. Nagore, L (Trad.). Papeles (94). Disponible en:http://www.hugoperezidiart.com.ar/teoria-aplicada-2014/Kaldor-2006.pdf Consultado: 10/05/2016

Kaldor, M. (2001). Las nuevas guerras. Violencia organizada en la era global. Barcelona, Tusquets.

Ramonet, I (2003). "Cumbre Digital en Ginebra". En: Revista La Isignia. Ciencia y Tecnología. España. 14 de diciembre de 2003. Disponible en: http://www.lainsignia.org/2003/diciembre/cyt_005.htm Consultado: 10/09/2016

Rodriguez, Gladys Stella (2005).Cumbre mundial sobre la sociedad de la información: Desafíos. Frónesis: Vol. 12, No. 2, 2005: 37 - 61. ISSN 1315-6268. Disponible en: http://www.scielo.org.ve/pdf/frone/v12n2/art04.pdf Consultado 01/09/2016

Serbin, A (2010): OEA y UNASUR: Seguridad regional y sociedad civil en América Latina 2010. Documentos CRIES (14),Buenos aires. Disponible en: http://www.cries.org/wp-content/uploads/2010/05/Documentos-14.pdf Consultado: 10/05/2016

Tortosa, J. (2005) La Palabra terrorista Recuperado de http://www.seipaz.org/2005tortosa.htm Consultado 1/10/2016

Wæver,O. (2009).Paz y seguridad: Dos conceptos en evolución y su relación cambiante. En: Günter Brauch, H., Oswald Spring, U. (Eds.) Reconceptualizar la seguridad en el siglo XXI. México: CIICH, Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades. 71-100. Disponible en: http://bibliotecavirtual.clacso.org.ar/Mexico/crim-unam/20100329020502/Reconceptualizarlaseguridad.pdf Consultado: 10/05/2016